日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

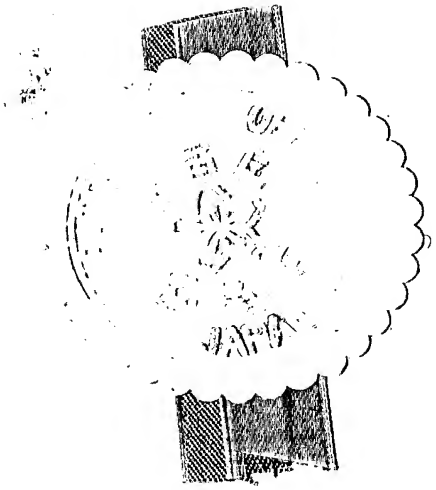
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００４年　１月２１日

出 願 番 号
Application Number: 特願２００４－０１３４０１

[ST. 10/C]: ［ＪＰ２００４－０１３４０１］

出 願 人
Applicant(s): シャープ株式会社
田中　初一



２００４年　２月２５日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００４－３０１３５１８

【書類名】　特許願
【整理番号】　03J05215
【提出日】　平成16年 1月21日
【あて先】　特許庁長官　殿
【国際特許分類】　H04L 9/02
H04L 9/14
G06F 7/72
G09C 1/00
【発明者】
【住所又は居所】　大阪府大阪市阿倍野区長池町２２番２２号　シャープ株式会社内
【氏名】　今井　繁規
【発明者】
【住所又は居所】　大阪府大阪市阿倍野区長池町２２番２２号　シャープ株式会社内
【氏名】　永井　知幸
【発明者】
【住所又は居所】　兵庫県神戸市須磨区中落合４丁目２－４６７－３０２
【氏名】　田中　初一
【特許出願人】
【識別番号】　000005049
【氏名又は名称】　シャープ株式会社
【特許出願人】
【識別番号】　503034629
【氏名又は名称】　田中　初一
【代理人】
【識別番号】　100080034
【弁理士】
【氏名又は名称】　原　謙三
【電話番号】　06-6351-4384
【選任した代理人】
【識別番号】　100113701
【弁理士】
【氏名又は名称】　木島　隆一
【選任した代理人】
【識別番号】　100116241
【弁理士】
【氏名又は名称】　金子　一郎
【先の出願に基づく優先権主張】
【出願番号】　特願2003- 16761
【出願日】　平成15年 1月24日
【手数料の表示】
【予納台帳番号】　003229
【納付金額】　21,000円
【提出物件の目録】
【物件名】　特許請求の範囲　1
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　0316194

【書類名】特許請求の範囲
【請求項１】
２つの素数ｐ，ｑを秘密鍵として生成し、その積ｎ＝ｐｑと、２つの乱数ｓ，ｔと、整数にｍｏｄｎの演算を施して得られる乗法群の最大生成源ｇとを用いて下記の関係式（１），（２）で表されるｇ１，ｇ２を公開鍵として生成する鍵生成手段と、
入力された平文ｍに対して、上記公開鍵｛ｇ１，ｇ２｝、秘密鍵ｎおよび乱数ｒ１，ｒ２を用いて、下記の関係式（３），（４）で表される暗号文Ｃ＝（Ｃ１，Ｃ２）を生成する暗号化演算手段とを備えたことを特徴とする暗号化装置。

$$g_1 = g^{s(p-1)} \pmod{n} \quad \cdots\cdots (1)$$
$$g_2 = g^{t(q-1)} \pmod{n} \quad \cdots\cdots (2)$$
$$C_1 = m \cdot g_1^{r_1} \pmod{n} \quad \cdots\cdots (3)$$
$$C_2 = m \cdot g_2^{r_2} \pmod{n} \quad \cdots\cdots (4)$$

（ただし、ｇｃｄ｛ｓ，ｑ－１｝＝１、ｇｃｄ｛ｔ，ｐ－１｝＝１とする）
【請求項２】
素数ｐ，ｑのうちｐを秘密鍵として生成し、その積ｎ＝ｐｑと、乱数ｓと、整数にｍｏｄｎの演算を施して得られる乗法群の最大生成源ｇとを用いて下記の関係式（１）で表されるｇ１を公開鍵として生成する鍵生成手段と、
入力された平文ｍに対して、上記公開鍵ｇ１、秘密鍵ｎおよび乱数ｒを用いて、下記の関係式（３）’で表される暗号文Ｃを生成する暗号化演算手段とを備えたことを特徴とする暗号化装置。

$$g_1 = g^{s(p-1)} \pmod{n} \quad \cdots\cdots (1)$$
$$C = m \cdot g_1^{r} \pmod{n} \quad \cdots\cdots (3)'$$

（ただし、情報ｂ＝size of ｐ (bits) であって、$0 < m < 2^{b-1}$、ｇｃｄ｛ｓ，ｑ－１｝＝１とする）
【請求項３】
上記暗号文Ｃに下記の関係式で示されるｅを加えて、Ｃ＝（Ｃ１，Ｃ２，ｅ）とすることを特徴とする請求項１に記載の暗号化装置。
（ただし、ｅ＝ｈ（ｄ）（ｈは一方向性ハッシュ関数）、ｄ＝（Ｃ１＋Ｃ２）／ｍ（ｍｏｄｎ）、$C_1 = m \cdot g_1^{r_1} \pmod{n}$、$C_2 = m \cdot g_2^{r_2} \pmod{n}$とする。）
【請求項４】
上記暗号文Ｃの乱数部分の計算を行ったデータを蓄積したデータベースを備えていることを特徴とする請求項１または３に記載の暗号化装置。
【請求項５】
上記暗号化演算手段は、最初の平文m_1だけを暗号文C_1＝（C_{11}，C_{12}）に暗号化し、それ以降の暗号文については、受信した平文m_iと、平文m_1のビット情報と、暗号文C_1に含まれる２つの乱数R_1またはR_2とを使用して暗号文を作成することを特徴とする請求項１または３に記載の暗号化装置。
【請求項６】
２つの素数ｐ，ｑを秘密鍵として生成し、その積ｎ＝ｐｑと、２つの乱数ｓ，ｔと、整数にｍｏｄｎの演算を施して得られる乗法群の最大生成源ｇとを用いて下記の関係式（１），（２）で表されるｇ１，ｇ２を公開鍵として用いるとともに、上記公開鍵｛ｇ１，ｇ２｝、秘密鍵ｎおよび乱数ｒ１，ｒ２を用いて、下記の関係式（３），（４）で表される平文ｍを暗号化した暗号文Ｃ＝（Ｃ１，Ｃ２）を受信し、
フェルマーの小定理を用いて下記の関係式（５），（６）で表される受信暗号文ａ，ｂを生成し、該受信暗号文ａ，ｂから、中国人剰余定理を用いて、下記の関係式（７）を満たす平文ｍを導出し、復号化処理を行う復号化演算手段を備えていることを特徴とする復号化装置。

$$g_1 = g^{s(p-1)} \pmod{n} \quad \cdots\cdots (1)$$
$$g_2 = g^{t(q-1)} \pmod{n} \quad \cdots\cdots (2)$$
$$C_1 = m \cdot g_1^{r_1} \pmod{n} \quad \cdots\cdots (3)$$

$C_2 = m \cdot g_2^{r_2} \pmod n$　・・・・・（4）
$a = C_1 \pmod p = m \pmod p$　・・・・・（5）
$b = C_2 \pmod q = m \pmod q$　・・・・・（6）
$m = aAq + bBp \pmod n$　・・・・・（7）
（ただし、$gcd\{s, q-1\} = 1$、$gcd\{t, p-1\} = 1$、$Aq \pmod p = 1$、$Bp \pmod q = 1$とする）

【請求項７】

素数ｐ，ｑのうちｐを秘密鍵として生成し、その積ｎ＝ｐｑと、乱数ｓと、整数にｍｏｄｎの演算を施して得られる乗法群の最大生成源ｇとを用いて下記の関係式（１）で表されるｇ１を公開鍵として生成し、入力された平文ｍに対して、上記公開鍵ｇ１、秘密鍵ｎおよび乱数ｒを用いて、下記の関係式（３）’で表される暗号文Ｃを受信し、

フェルマーの小定理を用いて下記の関係式（８）を満たす平文ｍを導出し、復号化処理を行う復号化演算手段を備えていることを特徴とする復号化装置。

$g_1 = g^{s(p-1)} \pmod n$　・・・・・（1）
$C = m \cdot g_1^{r} \pmod n$　・・・・・（3）’
$m = C \pmod p$　・・・・・（8）
（ただし、$gcd\{s, q-1\} = 1$とする）

【請求項８】

２つの素数ｐ，ｑを秘密鍵として生成し、その積ｎ＝ｐｑと、２つの乱数ｓ，ｔと、整数にｍｏｄｎの演算を施して得られる乗法群の最大生成源ｇとを用いて下記の関係式（１），（２）で表されるｇ１，ｇ２を公開鍵として生成する鍵生成手段と、入力された平文ｍに対して、上記公開鍵｛ｇ１，ｇ２｝、秘密鍵ｎおよび乱数ｒ１，ｒ２を用いて、下記の関係式（３），（４）で表される暗号文Ｃ１，Ｃ２を生成する暗号化演算手段とを備えた暗号化装置と、

上記暗号化装置で算出された暗号文Ｃ１，Ｃ２を受信し、フェルマーの小定理を用いて下記の関係式（５），（６）で表される受信暗号文ａ，ｂを生成し、該受信暗号文ａ，ｂから、中国人剰余定理を用いて、下記の関係式（７）を満たす平文ｍを導出し、復号化処理を行う復号化演算手段を備えている復号化装置とを備えていることを特徴とする暗号システム。

$g_1 = g^{s(p-1)} \pmod n$　・・・・・（1）
$g_2 = g^{t(q-1)} \pmod n$　・・・・・（2）
$C_1 = m \cdot g_1^{r_1} \pmod n$　・・・・・（3）
$C_2 = m \cdot g_2^{r_2} \pmod n$　・・・・・（4）
$a = C_1 \pmod p = m \pmod p$　・・・・・（5）
$b = C_2 \pmod q = m \pmod q$　・・・・・（6）
$m = aAq + bBp \pmod n$　・・・・・（7）
（ただし、$gcd\{s, q-1\} = 1$、$gcd\{t, p-1\} = 1$、$Aq \pmod p = 1$、$Bp \pmod q = 1$とする）

【請求項９】

素数ｐ，ｑのうちｐを秘密鍵として生成し、その積ｎ＝ｐｑと、乱数ｓと、整数にｍｏｄｎの演算を施して得られる乗法群の最大生成源ｇとを用いて下記の関係式（１）で表されるｇ１を公開鍵として生成する鍵生成手段と、入力された平文ｍに対して、上記公開鍵ｇ１、秘密鍵ｎおよび乱数ｒを用いて、下記の関係式（３）’で表される暗号文Ｃを生成する暗号化演算手段とを有する暗号化装置と、

上記暗号化装置から暗号文Ｃを受信し、フェルマーの小定理を用いて下記の関係式（８）を満たす平文ｍを導出し、復号化処理を行う復号化演算手段を有する復号化装置とを備えていることを特徴とする暗号システム。

$g_1 = g^{s(p-1)} \pmod n$　・・・・・（1）
$C = m \cdot g_1^{r} \pmod n$　・・・・・（3）’
$m = C \pmod p$　・・・・・（8）

（ただし、ｇｃｄ｛ｓ，ｑ－１｝＝１とする）

【請求項１０】

２つの素数ｐ，ｑを秘密鍵として生成し、その積ｎ＝ｐｑと、２つの乱数ｓ，ｔと、整数にｍｏｄｎの演算を施して得られる乗法群の最大生成源ｇとを用いて下記の関係式（１），（２）で表されるｇ$_1$，ｇ$_2$を公開鍵として生成するとともに、

入力された平文ｍに対して、上記公開鍵｛ｇ$_1$，ｇ$_2$｝、秘密鍵ｎおよび乱数ｒ１，ｒ２を用いて、下記の関係式（３），（４）で表される暗号文Ｃ$_1$，Ｃ$_2$を生成することを特徴とする暗号化方法。

$$g_1 = g^{s(p-1)} \pmod n \quad \cdots\cdots (1)$$

$$g_2 = g^{t(q-1)} \pmod n \quad \cdots\cdots (2)$$

$$C_1 = m \cdot g_1^{r1} \pmod n \quad \cdots\cdots (3)$$

$$C_2 = m \cdot g_2^{r2} \pmod n \quad \cdots\cdots (4)$$

（ただし、ｇｃｄ｛ｓ，ｑ－１｝＝１、ｇｃｄ｛ｔ，ｐ－１｝＝１とする）

【請求項１１】

素数ｐ，ｑのうちｐを秘密鍵として生成し、その積ｎ＝ｐｑと、乱数ｓと、整数にｍｏｄｎの演算を施して得られる乗法群の最大生成源ｇとを用いて下記の関係式（１）で表されるｇ$_1$を公開鍵として生成するとともに、

入力された平文ｍに対して、上記公開鍵ｇ$_1$、秘密鍵ｎおよび乱数ｒを用いて、下記の関係式（３）’で表される暗号文Ｃを生成することを特徴とする暗号化方法。

$$g_1 = g^{s(p-1)} \pmod n \quad \cdots\cdots (1)$$

$$C = m \cdot g_1^{r} \pmod n \quad \cdots\cdots (3)'$$

（ただし、情報ｂ＝size of ｐ（bits）であって、$0 < m < 2^{b-1}$，ｇｃｄ｛ｓ，ｑ－１｝＝１とする）

【請求項１２】

２つの素数ｐ，ｑを秘密鍵として生成し、その積ｎ＝ｐｑと、２つの乱数ｓ，ｔと、整数にｍｏｄｎの演算を施して得られる乗法群の最大生成源ｇとを用いて下記の関係式（１），（２）で表されるｇ$_1$，ｇ$_2$を公開鍵として用いるとともに、上記公開鍵｛ｇ$_1$，ｇ$_2$｝、秘密鍵ｎおよび乱数ｒ１，ｒ２を用いて、下記の関係式（３），（４）で表される平文ｍを暗号化した暗号文Ｃ＝（Ｃ$_1$，Ｃ$_2$）を受信し、

フェルマーの小定理を用いて下記の関係式（５），（６）で表される受信暗号文ａ，ｂを生成し、該受信暗号文ａ，ｂから、中国人剰余定理を用いて、下記の関係式（７）を満たす平文ｍを導出し、復号化処理を行うことを特徴とする復号化方法。

$$g_1 = g^{s(p-1)} \pmod n \quad \cdots\cdots (1)$$

$$g_2 = g^{t(q-1)} \pmod n \quad \cdots\cdots (2)$$

$$C_1 = m \cdot g_1^{r1} \pmod n \quad \cdots\cdots (3)$$

$$C_2 = m \cdot g_2^{r2} \pmod n \quad \cdots\cdots (4)$$

$$a = C_1 \pmod p = m \pmod p \quad \cdots\cdots (5)$$

$$b = C_2 \pmod q = m \pmod q \quad \cdots\cdots (6)$$

$$m = aAq + bBp \pmod n \quad \cdots\cdots (7)$$

（ただし、ｇｃｄ｛ｓ，ｑ－１｝＝１、ｇｃｄ｛ｔ，ｐ－１｝＝１、Ａｑ（ｍｏｄｐ）＝１、Ｂｐ（ｍｏｄｑ）＝１とする）

【請求項１３】

素数ｐ，ｑのうちｐを秘密鍵として生成し、その積ｎ＝ｐｑと、乱数ｓと、整数にｍｏｄｎの演算を施して得られる乗法群の最大生成源ｇを用いて下記の関係式（１）で表されるｇ$_1$とを公開鍵として生成し、入力された平文ｍに対して、上記公開鍵ｇ$_1$、秘密鍵ｎおよび乱数ｒを用いて、下記の関係式（３）’で表される暗号文Ｃを受信し、

フェルマーの小定理を用いて下記の関係式（８）を満たす平文ｍを導出し、復号化処理を行うことを特徴とする復号化方法。

$$g_1 = g^{s(p-1)} \pmod n \quad \cdots\cdots (1)$$

$$C = m \cdot g_1^{r} \pmod n \quad \cdots\cdots (3)'$$

$$m = C \pmod{p} \quad \cdots\cdots (8)$$

（ただし、ｇｃｄ｛ｓ，ｑ－１｝＝１とする）

【書類名】明細書
【発明の名称】暗号化装置および復号化装置、並びにこれらを備えた暗号システム、暗号化方法および復号化方法
【技術分野】
【０００１】
本発明は、インターネット等を通じて送受信される通信文を暗号化するための暗号化装置、および暗号化された通信文を復号化するための復号化装置、並びにこれらを備えた暗号システムに関するものである。
【背景技術】
【０００２】
従来より、インターネット等を通じてやり取りが行われるデータ等の漏洩、改竄が問題となっており、この対策として、データ等を暗号化して相手先へ送信する暗号システムが利用されている。
【０００３】
暗号システムは、共通鍵暗号方式と公開鍵暗号方式とに大別され、鍵管理の容易性、データ漏洩の危険性が低い等の理由から、主として、公開鍵暗号方式が採用されている。
【０００４】
公開鍵暗号方式の代表的な例としては、ＲＳＡ暗号化方式がある。
【０００５】
このＲＳＡ暗号化方式は、２つの素数ｐ，ｑを実質的な秘密鍵として生成し、その積ｎ＝ｐｑを公開鍵の一つとして用いることで、ｐｑからｎは容易に求められるが、ｎから２つの素数ｐ，ｑを求めることが非常に困難であるという性質を利用した公開鍵暗号方式である。
【０００６】
このように、ｎを公開鍵の一つとして公開することで、誰もが暗号文を作成できる一方、これを復号するために２つの大きな素数ｐ，ｑを求めることは非常に困難であることから、ＲＳＡ暗号化方式によって送信されるデータの安全性は非常に高いといえる。
【特許文献１】特開平８－２５１１５５号公報（１９９６年９月２７日公開）
【特許文献２】特開２０００－２１４７７７号公報（２０００年８月４日公開）
【発明の開示】
【発明が解決しようとする課題】
【０００７】
しかしながら、上述のような従来のＲＳＡ暗号化方式では、データの秘匿性の面では高い性能を有し、アルゴリズムも単純であるものの、その安全性は大きな二つの素数ｐ，ｑの積ｎを素因数分解する困難さに起因している。このため、ｎ＝ｐｑの値を10進法で200桁程度の大きさにする必要があり、暗号化および復号を実行するために必要なｎを法とするべき乗計算の実行が極めて困難であるという問題を有している。
【０００８】
さらに、ＲＳＡ暗号化方式は、乗法特性を有しており、２つの署名から第３の署名が生成できるため、安全性の面で問題がある。
【０００９】
本発明は、上記の問題点に鑑みてなされたものであり、その目的は、極めて簡単な秘密暗号系を提案し、ＲＳＡ暗号化方式と等価な安全性を保持しつつ、アルゴリズムをより単純化し、簡単な計算で暗号化および復号化が可能な暗号化装置および復号化装置、並びにこれらを備えた暗号システム、暗号化方法および復号化方法を提供することにある。
【課題を解決するための手段】
【００１０】
本発明の暗号化装置は、上記の課題を解決するために、２つの素数ｐ，ｑを秘密鍵として生成し、その積ｎ＝ｐｑと、２つの乱数ｓ，ｔと、整数にｍｏｄｎの演算を施して得られる乗法群の最大生成源ｇとを用いて下記の関係式（１）、（２）で表されるｇ$_1$，ｇ$_2$

を公開鍵として生成する鍵生成手段と、入力された平文ｍに対して、上記公開鍵｛g_1，g_2｝、秘密鍵ｎおよび乱数ｒ１，ｒ２を用いて、下記の関係式（３）、（４）で表される暗号文Ｃ＝（C_1、C_2）を生成する暗号化演算手段とを備えたことを特徴としている。

$g_1 = g^{s(p-1)} \pmod n$　・・・・・（１）

$g_2 = g^{t(q-1)} \pmod n$　・・・・・（２）

$C_1 = m \cdot g_1^{r1} \pmod n$　・・・・・（３）

$C_2 = m \cdot g_2^{r2} \pmod n$　・・・・・（４）

（ただし、ｇｃｄ｛ｓ，ｑ－１｝＝１、ｇｃｄ｛ｔ，ｐ－１｝＝１とする）。

【００１１】

上記の構成によれば、公開鍵として生成した鍵g_1，g_2は、それぞれ（ｐ－１），（ｑ－１）のべき乗を含んでおり、公開鍵｛g_1，g_2｝及び秘密鍵ｎを用いて生成した暗号文C_1，C_2も、（ｐ－１），（ｑ－１）のべき乗をそれぞれ含んでいるため、この暗号文C_1，C_2を復号化する際において、フェルマーの小定理（$a^{p-1} \equiv 1 \pmod p$））を用いて、簡単に復号化することができる。

【００１２】

すなわち、本発明の暗号化装置は、鍵生成手段により、２つの大きな素数ｐ，ｑを発生させ、これを秘密鍵として用いるとともに、この秘密鍵｛ｐ，ｑ｝と乱数ｓ，ｔとを用いて、それぞれ（ｐ－１），（ｑ－１）のべき乗を含むように公開鍵｛g_1，g_2｝を生成している。

【００１３】

これにより、２つの大きな素数ｐ，ｑをそのまま秘密鍵として用いることができ、さらに、公開鍵｛g_1，g_2｝についても、乱数を用いて、（ｐ－１）のべき乗を含む非常に簡単な計算で算出できる。

【００１４】

また、本発明の暗号化装置の暗号化演算手段によって生成された暗号文は、公開鍵｛g_1，g_2｝及び秘密鍵ｎを用いて、（ｐ－１），（ｑ－１）のべき乗を含んだ式で表されるため、その復号化にはフェルマーの小定理を用いることが可能になる。

【００１５】

フェルマーの小定理は、$a^{p-1} \equiv 1 \pmod p$で表され、（ｐ－１）のべき乗を含む数に対して、ｍｏｄｐの演算を施すことでその剰余を「１」に帰着させることができる。よって、暗号文C_1，C_2から、フェルマーの小定理を用いて、暗号文C_1，C_2に対応する２つの受信暗号文を算出し、ここでさらに中国人剰余定理を用いることで、２つの受信暗号文から平文ｍを復号化できる。

【００１６】

本発明の暗号化装置では、以上のように、単純な秘密鍵｛ｐ，ｑ｝を用いて、簡単な計算で公開鍵｛g_1，g_2｝、秘密鍵ｎを生成し、暗号文も簡単な計算で算出でき、さらにこの暗号文の復号化についても、フェルマーの小定理を用いて簡単に計算できるため、従来の暗号化方式と比較して、高速処理が可能になる。

【００１７】

一方、本発明の暗号化装置における安全性については、公開鍵｛g_1，g_2｝には、それぞれ乱数ｓ，ｔが含まれているため、公開鍵｛g_1，g_2｝及び秘密鍵ｎは互いに関係が断ち切られている。

【００１８】

よって、本発明の暗号化装置によれば、高い安全性を維持しつつ、計算量を減らして暗号化および復号化の高速処理を行うことが可能になる。

【００１９】

本発明の暗号化装置は、上記の課題を解決するために、素数ｐ，ｑのうちｐを秘密鍵として生成し、その積ｎ＝ｐｑと、乱数ｓと、整数にｍｏｄｎの演算を施して得られる乗法群の最大生成源ｇとを用いて下記の関係式（１）で表されるg_1を公開鍵として生成する

鍵生成手段と、入力された平文mに対して、上記公開鍵g_1、秘密鍵nおよび乱数rを用いて、下記の関係式（３）’で表される暗号文Cを生成する暗号化演算手段とを備えたことを特徴としている。

$g_1 = g^{s(p-1)} \pmod n$　・・・・・（１）

$C = m \cdot g_1^{r} \pmod n$　・・・・・（３）’

（ただし、情報b＝size of p (bits) であって、$0 < m < 2^{b-1}$，gcd｛s，q－1｝＝1とする）

上記の構成によれば、公開鍵として生成した鍵g_1は、（p－1）のべき乗を含んでおり、公開鍵g_1及び秘密鍵nを用いて生成した暗号文Cも、（p－1）のべき乗を含んでいるため、フェルマーの小定理（$a^{p-1} \equiv 1 \pmod p$）を用いて、この暗号文Cを簡単に復号化することができる。

【００２０】

すなわち、本発明の暗号化装置は、鍵生成手段により、２つの大きな素数p，qを発生させ、これを秘密鍵として用いるとともに、この秘密鍵｛p，q｝と乱数s，tとを用いて、それぞれ（p－1）のべき乗を含むように公開鍵g_1を生成している。

【００２１】

さらに、秘密鍵pのサイズbとの関係において、メッセージmに長さの制限を課し、このサイズbを用いることで、暗号文の生成および復号化の計算をそれぞれ１つの式で行うことができるため、中国人剰余定理を用いることなく、より簡単な計算により暗号化復号化処理を行うことができる。

【００２２】

また、本発明の暗号化装置の暗号化演算手段によって生成された暗号文は、上記と同様に、公開鍵g_1及び秘密鍵nを用いて、（p－1）のべき乗を含んだ式で表されるため、その復号化にはフェルマーの小定理を用いることが可能である。

【００２３】

フェルマーの小定理は、$a^{p-1} \equiv 1 \pmod p$で表され、（p－1）のべき乗を含む数に対して、modpの演算を施すことでその剰余を「１」に帰着させることができる。

【００２４】

よって、単純な秘密鍵｛p，q｝を用いて、簡単な計算で公開鍵g_1を生成し、暗号文も簡単な計算で算出でき、さらにこの暗号文の復号化についても、フェルマーの小定理だけを用いることで簡単に計算できるため、従来の暗号化方式と比較して、さらに高速処理が可能になる。

【００２５】

一方、本発明の暗号化装置における安全性については、公開鍵g_1には、乱数sが含まれているため、公開鍵g_1及び秘密鍵nは互いに関係が断ち切られている。

【００２６】

よって、本発明の暗号化装置によれば、高い安全性を維持しつつ、平文mの長さに制限を加えることで、さらに計算量を減らして暗号化、復号化処理の高速化を実現できる。

【００２７】

上記暗号文Cに下記の関係式で示されるeを加えて、C＝（C_1，C_2，e）とすることがより好ましい。（ただし、e＝h（d）（hは一方向性ハッシュ関数）、d＝（C_1＋C_2）／m（modn）、$C_1 = m \cdot g_1^{r1} \pmod n$，$C_2 = m \cdot g_2^{r2} \pmod n$とする）。

【００２８】

これにより、暗号文Cが長くなるが、メッセージmが少しでも変わるとeが一致しなくなるため、適応型選択暗号文攻撃（ＣＣＡ２）に対しても耐性を持たせて、より信頼度の高い暗号システムを得ることができる。

【００２９】

また、eはハッシュ関数を用いて計算されているため、３２bitsまたは６４bits程度の

情報量にまとめることができる。

【００３０】

上記暗号文Ｃの乱数部分の計算を行ったデータを蓄積したデータベースを備えていることがより好ましい。

【００３１】

これにより、例えば、暗号文Ｃに含まれる乱数部分のデータを蓄積した２行ｆ列のデータベースを予め用意しておくことで、暗号化処理を行う際には、このデータベースから対応する乱数を取り出して暗号文を作成することができるため、暗号化処理をより高速化できる。

【００３２】

よって、例えば、従来のＲＳＡ暗号方式と比較して、計算量を減らして暗号化処理を高速化できるとともに、復号化処理についてもｍｏｄｐの演算を施すだけで復号化できるため、計算量が多い従来のＲＳＡ暗号化方式の暗号システムと比較してはるかに高速化できる。

【００３３】

上記暗号化演算手段は、最初の暗号文Ｃだけを暗号文C_1，C_2に暗号化し、それ以降の暗号文については前の暗号文C_1と、C_1に含まれる２つの乱数とを使用して暗号文を作成することがより好ましい

これにより、最初の暗号文Ｃについてのみ通常の手順で暗号文を作成し、それ以降の暗号文については、最初のビットb_i＝０の場合には、乱数部分R_1を加算し、最初のビットb_i＝１の場合には、乱数部分R_2を加算していくことで、暗号文Ｃを作成できる。

【００３４】

本発明の復号化装置は、上記の課題を解決するために、２つの素数ｐ，ｑを秘密鍵として生成し、その積ｎ＝ｐｑと、２つの乱数ｓ，ｔと、整数にｍｏｄｎの演算を施して得られる乗法群の最大生成源ｇとを用いて下記の関係式（１），（２）で表されるg_1，g_2を公開鍵として用いるとともに、上記公開鍵｛g_1，g_2｝、秘密鍵ｎおよび乱数ｒ１，ｒ２を用いて、下記の関係式（３），（４）で表される平文ｍを暗号化した暗号文Ｃ＝（C_1，C_2）を受信し、フェルマーの小定理を用いて下記の関係式（５），（６）で表される受信暗号文ａ，ｂを生成し、該受信暗号文ａ，ｂから、中国人剰余定理を用いて、下記の関係式（７）を満たす平文ｍを導出し、復号化処理を行う復号化演算手段を備えていることを特徴としている。

$g_1 = g^{s(p-1)} \pmod n$　・・・・・（１）

$g_2 = g^{t(q-1)} \pmod n$　・・・・・（２）

$C_1 = m \cdot g_1^{r1} \pmod n$　・・・・・（３）

$C_2 = m \cdot g_2^{r2} \pmod n$　・・・・・（４）

$a = C_1 \pmod p = m \pmod p$　・・・・・（５）

$b = C_2 \pmod q = m \pmod q$　・・・・・（６）

$m = aAq + bBp \pmod n$　・・・・・（７）

（ただし、$gcd\{s, q-1\} = 1$、$gcd\{t, p-1\} = 1$、$Aq \pmod p = 1$、$Bp \pmod q = 1$とする）。

【００３５】

上記の構成によれば、公開鍵として生成した鍵g_1，g_2は、それぞれ（ｐ－１），（ｑ－１）のべき乗を含んでおり、公開鍵｛g_1，g_2｝及び秘密鍵ｎを用いて生成した暗号文C_1，C_2も、（ｐ－１），（ｑ－１）のべき乗をそれぞれ含んでいるため、この暗号文C_1，C_2を復号化する際において、フェルマーの小定理（$a^{p-1} \equiv 1 \pmod p$））を用いて、簡単に復号化することができる。

【００３６】

すなわち、本発明の復号化装置が受信する暗号文は、公開鍵｛g_1，g_2｝及び秘密鍵ｎを用いて、（ｐ－１），（ｑ－１）のべき乗を含んだ式で表されるため、その復号化にはフェルマーの小定理を用いることが可能になる。

【００３７】
フェルマーの小定理は、$a^{p-1} \equiv 1$（ｍｏｄｐ）で表され、（ｐ－１）のべき乗を含む数に対して、ｍｏｄｐの演算を施すことでその剰余を「１」に帰着させることができる。よって、暗号文C_1，C_2から、フェルマーの小定理を用いて、暗号文C_1，C_2に対応する２つの受信暗号文を算出し、ここでさらに中国人剰余定理を用いることで、２つの受信暗号文から平文ｍを復号化できる。

【００３８】
以上のように、本発明の復号化装置では、フェルマーの小定理を用いて簡単に暗号文を復号化できるため、従来の復号化方式と比較して、高速処理が可能になる。

【００３９】
本発明の復号化装置は、上記の課題を解決するために、素数ｐ，ｑのうちｐを秘密鍵として生成し、その積$n = pq$と、乱数ｓと、整数にｍｏｄｎの演算を施して得られる乗法群の最大生成源ｇとを用いて下記の関係式（１）で表されるｇ１を公開鍵として生成し、入力された平文ｍに対して、上記公開鍵ｇ１、秘密鍵ｎおよび乱数ｒを用いて、下記の関係式（３）’で表される暗号文Ｃを受信し、

フェルマーの小定理を用いて下記の関係式（８）を満たす平文ｍを導出し、復号化処理を行う復号化演算手段を備えていることを特徴としている。

$g_1 = g^{s(p-1)}$（ｍｏｄｎ）　・・・・・（１）

$C = m \cdot g_1^{r}$（ｍｏｄｎ）　・・・・・（３）’

$m = C$（ｍｏｄｐ）　・・・・・（８）

（ただし、$gcd\{s, q-1\} = 1$とする）。

【００４０】
上記の構成によれば、公開鍵ｇ１を用いて生成した暗号文Ｃは、（ｐ－１）のべき乗を含んでいるため、フェルマーの小定理（$a^{p-1} \equiv 1$（ｍｏｄｐ））を用いて、この暗号文Ｃを簡単に復号化することができる。

【００４１】
すなわち、本発明の復号化装置は、秘密鍵ｐのサイズｂとの関係において、メッセージｍに長さの制限を課し、このサイズｂを用いることで、暗号文Ｃの生成および復号化の計算をそれぞれ１つの式で行うことができるため、中国人剰余定理を用いることなく、より簡単な計算により復号化処理を行うことができる。

【００４２】
また、本発明の復号化装置で復号化される暗号文は、公開鍵ｇ１を用いて、（ｐ－１）のべき乗を含んだ式で表されるため、その復号化にはフェルマーの小定理を用いることが可能である。

【００４３】
フェルマーの小定理は、$a^{p-1} \equiv 1$（ｍｏｄｐ）で表され、（ｐ－１）のべき乗を含む数に対して、ｍｏｄｐの演算を施すことでその剰余を「１」に帰着させることができる。

【００４４】
よって、単純な秘密鍵｛ｐ，ｑ｝を用いて、簡単な計算で公開鍵ｇ１及び秘密鍵ｎを生成し、暗号文も簡単な計算で算出でき、さらに暗号文の復号化についても、フェルマーの小定理だけを用いることで簡単に計算できるため、従来の復号化方式と比較して、さらに高速処理が可能になる。

【００４５】
なお、本発明は、暗号鍵の配布に適用することが可能である。

【００４６】
本発明の暗号システムは、上記の課題を解決するために、２つの素数ｐ，ｑを秘密鍵として生成し、その積$n = pq$と、２つの乱数ｓ，ｔと、整数にｍｏｄｎの演算を施して得られる乗法群の最大生成源ｇとを用いて下記の関係式（１），（２）で表されるｇ１，ｇ２を公開鍵として生成する鍵生成手段と、入力された平文ｍに対して、上記公開鍵｛ｇ１

，g_2｝、秘密鍵ｎおよび乱数ｒ１，ｒ２を用いて、下記の関係式（３），（４）で表される暗号文C_1，C_2を生成する暗号化演算手段とを備えた暗号化装置と、上記暗号化装置で算出された暗号文C_1，C_2を受信し、フェルマーの小定理を用いて下記の関係式（５），（６）で表される受信暗号文ａ，ｂを生成し、該受信暗号文ａ，ｂから、中国人剰余定理を用いて、下記の関係式（７）を満たす平文ｍを導出し、復号化処理を行う復号化演算手段を備えている復号化装置とを備えていることを特徴としている。

$g_1 = g^{s(p-1)} \pmod n$　・・・・・（１）

$g_2 = g^{t(q-1)} \pmod n$　・・・・・（２）

$C_1 = m \cdot g_1^{r1} \pmod n$　・・・・・（３）

$C_2 = m \cdot g_2^{r2} \pmod n$　・・・・・（４）

$a = C_1 \pmod p = m \pmod p$　・・・・・（５）

$b = C_2 \pmod q = m \pmod q$　・・・・・（６）

$m = aAq + bBp \pmod n$　・・・・・（７）

（ただし、$gcd\{s, q-1\} = 1$、$gcd\{t, p-1\} = 1$、$Aq \pmod p = 1$、$Bp \pmod q = 1$とする）。

【００４７】

上記の構成によれば、暗号化装置において、公開鍵として生成した鍵g_1，g_2は、それぞれ（ｐ－１），（ｑ－１）のべき乗を含んでおり、公開鍵｛g_1，g_2｝及び秘密鍵ｎを用いて生成した暗号文C_1，C_2も、（ｐ－１），（ｑ－１）のべき乗をそれぞれ含んでいるため、復号化装置において、フェルマーの小定理（$a^{p-1} \equiv 1 \pmod p$）を用いて、暗号文C_1，C_2を簡単に復号化することができる。

【００４８】

すなわち、本発明の暗号システムは、暗号化装置と復号化装置とを備えている。暗号化装置は、鍵生成手段を備え、２つの大きな素数ｐ，ｑを発生させ、これを秘密鍵として用いるとともに、この秘密鍵｛ｐ，ｑ｝と乱数ｓ，ｔとを用いて、それぞれ（ｐ－１），（ｑ－１）のべき乗を含むように公開鍵｛g_1，g_2｝を生成している。

【００４９】

これにより、２つの大きな素数ｐ，ｑをそのまま秘密鍵として用いることができ、さらに、公開鍵｛g_1，g_2｝についても、乱数を用いて、（ｐ－１）のべき乗を含む非常に簡単な計算で算出できる。

【００５０】

また、本発明の暗号システムの暗号化装置は、暗号化演算手段において、公開鍵｛g_1，g_2｝を用いて、（ｐ－１），（ｑ－１）のべき乗を含んだ式で表される暗号文Ｃを作成するため、その暗号文Ｃの復号化にフェルマーの小定理を用いることが可能になる。

【００５１】

フェルマーの小定理は、$a^{p-1} \equiv 1 \pmod p$で表され、（ｐ－１）のべき乗を含む数に対して、ｍｏｄｐの演算を施すことでその剰余を「１」に帰着させることができる。よって、暗号文C_1，C_2から、フェルマーの小定理を用いて、暗号文C_1，C_2に対応する２つの受信暗号文を算出し、ここでさらに中国人剰余定理を用いることで、２つの受信暗号文から平文ｍを復号化できる。

【００５２】

以上のように、本発明の暗号システムでは、暗号化装置において、単純な秘密鍵｛ｐ，ｑ｝を用いて、簡単な計算で公開鍵｛g_1，g_2｝及び秘密鍵ｎを生成し、暗号文も簡単な計算で算出でき、さらに、復号化装置において、フェルマーの小定理を用いて簡易に暗号文を復号化できるため、従来の暗号システムと比較して、高速処理が可能になる。

【００５３】

一方、本発明の暗号システムにおける安全性については、暗号化装置において作成される公開鍵｛g_1，g_2｝には、それぞれ乱数ｓ，ｔが含まれているため、公開鍵｛g_1，g_2｝及び秘密鍵ｎは互いに関係が断ち切られている。

【００５４】

よって、本発明の暗号システムによれば、高い安全性を維持しつつ、計算量を減らして暗号化および復号化の高速処理を行うことが可能になる。

【００５５】

本発明の暗号システムは、上記の課題を解決するために、素数ｐ，ｑのうちｐを秘密鍵として生成し、その積ｎ＝ｐｑと、乱数ｓと、整数にｍｏｄｎの演算を施して得られる乗法群の最大生成源ｇとを用いて下記の関係式（１）で表されるｇ１を公開鍵として生成する鍵生成手段と、入力された平文ｍに対して、上記公開鍵ｇ１、秘密鍵ｎおよび乱数ｒを用いて、下記の関係式（３）’で表される暗号文Ｃを生成する暗号化演算手段とを有する暗号化装置と、上記暗号化装置から暗号文Ｃを受信し、フェルマーの小定理を用いて下記の関係式（８）を満たす平文ｍを導出し、復号化処理を行う復号化演算手段を有する復号化装置とを備えていることを特徴としている。

$g_1 = g^{s(p-1)} \pmod n$　・・・・・（１）

$C = m \cdot g_1^{r} \pmod n$　・・・・・（３）’

$m = C \pmod p$　・・・・・（８）

（ただし、ｇｃｄ｛ｓ，ｑ－１｝＝１とする）。

【００５６】

上記の構成によれば、暗号化装置において、公開鍵ｇ１及び秘密鍵ｎを用いて作成された暗号文Ｃは、（ｐ－１）のべき乗を含んでいるため、復号化装置において、フェルマーの小定理（$a^{p-1} \equiv 1 \pmod p$）を用いて、この暗号文Ｃを簡単に復号化することができる。

【００５７】

すなわち、本発明の暗号システムは、暗号化装置が備えている鍵生成手段により、２つの大きな素数ｐ，ｑを発生させ、これを秘密鍵として用いるとともに、この秘密鍵｛ｐ，ｑ｝と乱数ｓ，ｔとを用いて、それぞれ（ｐ－１）のべき乗を含むように公開鍵ｇ１を生成している。

【００５８】

さらに、秘密鍵ｐのサイズｂとの関係において、メッセージｍに長さの制限を課し、このサイズｂを用いることで、暗号文Ｃの生成および復号化の計算をそれぞれ１つの式で行うことができるため、復号化装置において、中国人剰余定理を用いることなく、より簡単な計算により復号化処理を行うことができる。

【００５９】

また、本発明の暗号システムにおいては、復号化装置において復号化される暗号文が、（ｐ－１）のべき乗を含んだ式で表されるため、その復号化にはフェルマーの小定理を用いることが可能である。

【００６０】

フェルマーの小定理は、$a^{p-1} \equiv 1 \pmod p$で表され、（ｐ－１）のべき乗を含む数に対して、ｍｏｄｐの演算を施すことでその剰余を「１」に帰着させることができる。

【００６１】

よって、単純な秘密鍵｛ｐ，ｑ｝を用いて、簡単な計算で公開鍵ｇ１及び秘密鍵ｎを生成し、暗号文も簡単な計算で算出でき、さらに暗号文の復号化についても、フェルマーの小定理だけを用いることで簡単に計算できるため、従来の復号化方式と比較して、さらに高速処理が可能になる。

【００６２】

一方、本発明の暗号システムにおける安全性については、公開鍵ｇ１には、乱数ｓが含まれているため、公開鍵ｇ１及び秘密鍵ｎは互いに関係が断ち切られている。

【００６３】

よって、本発明の暗号化装置によれば、高い安全性を維持しつつ、平文ｍの長さに制限を加えることで、さらに簡単な計算により暗号化、復号化処理を行って、高速処理を実現できる。

【００６４】

本発明の暗号化方法は、上記の課題を解決するために、２つの素数ｐ，ｑを秘密鍵として生成し、その積ｎ＝ｐｑと、２つの乱数ｓ，ｔと、整数にｍｏｄｎの演算を施して得られる乗法群の最大生成源ｇとを用いて下記の関係式（１），（２）で表されるｇ$_1$，ｇ$_2$を公開鍵として生成するとともに、入力された平文ｍに対して、上記公開鍵｛ｇ$_1$，ｇ$_2$｝、秘密鍵ｎおよび乱数ｒ１，ｒ２を用いて、下記の関係式（３），（４）で表される暗号文Ｃ$_1$，Ｃ$_2$を生成することを特徴としている。

$g_1 = g^{s(p-1)} \pmod n$　・・・・・（１）

$g_2 = g^{t(q-1)} \pmod n$　・・・・・（２）

$C_1 = m \cdot g_1^{r_1} \pmod n$　・・・・・（３）

$C_2 = m \cdot g_2^{r_2} \pmod n$　・・・・・（４）

（ただし、ｇｃｄ｛ｓ，ｑ－１｝＝１、ｇｃｄ｛ｔ，ｐ－１｝＝１とする）。

【００６５】

上記の暗号化方法によれば、公開鍵として生成した鍵ｇ$_1$，ｇ$_2$は、それぞれ（ｐ－１），（ｑ－１）のべき乗を含んでおり、公開鍵｛ｇ$_1$，ｇ$_2$｝及び秘密鍵ｎを用いて生成した暗号文Ｃ$_1$，Ｃ$_2$も、（ｐ－１），（ｑ－１）のべき乗をそれぞれ含んでいるため、この暗号文Ｃ$_1$，Ｃ$_2$を復号化する際において、フェルマーの小定理（$a^{p-1} \equiv 1 \pmod p$）を用いて、簡単に復号化することができる。

【００６６】

すなわち、本発明の暗号化方法は、２つの大きな素数ｐ，ｑを発生させ、これを秘密鍵として用いるとともに、この秘密鍵｛ｐ，ｑ｝と乱数ｓ，ｔとを用いて、それぞれ（ｐ－１），（ｑ－１）のべき乗を含むように公開鍵｛ｇ$_1$，ｇ$_2$｝を生成している。

【００６７】

これにより、２つの大きな素数ｐ，ｑをそのまま秘密鍵として用いることができ、さらに、公開鍵｛ｇ$_1$，ｇ$_2$｝についても、乱数を用いて非常に簡単な計算により算出できる。

【００６８】

また、本発明の暗号化方法によって生成された暗号文は、公開鍵｛ｇ$_1$，ｇ$_2$｝及び秘密鍵ｎを用いて、（ｐ－１），（ｑ－１）のべき乗を含んだ式で表されるため、その復号化にはフェルマーの小定理を用いることが可能になる。

【００６９】

フェルマーの小定理は、$a^{p-1} \equiv 1 \pmod p$で表され、（ｐ－１）のべき乗を含む数に対して、ｍｏｄｐの演算を施すことでその剰余を「１」に帰着させることができる。よって、暗号文Ｃ$_1$，Ｃ$_2$から、フェルマーの小定理を用いて、暗号文Ｃ$_1$，Ｃ$_2$に対応する２つの受信暗号文を算出し、ここでさらに中国人剰余定理を用いることで、２つの受信暗号文から平文ｍを復号化できる。

【００７０】

以上のように、本発明の暗号化方法では、単純な秘密鍵｛ｐ，ｑ｝を用いて、簡単な計算で公開鍵｛ｇ$_1$，ｇ$_2$｝及び秘密鍵ｎを生成し、暗号文も簡単な計算で算出でき、さらにこの暗号文の復号化についても、フェルマーの小定理を用いて簡単に計算できるため、従来の暗号化方法と比較して、高速処理が可能になる。

【００７１】

一方、本発明の暗号化方法における安全性については、公開鍵｛ｇ$_1$，ｇ$_2$｝には、それぞれ乱数ｓ，ｔが含まれているため、公開鍵｛ｇ$_1$，ｇ$_2$｝及び秘密鍵ｎは互いに関係が断ち切られている。

【００７２】

よって、本発明の暗号化方法によれば、高い安全性を維持しつつ、計算量を減らして暗号化および復号化の高速処理を行うことが可能になる。

【００７３】

本発明の暗号化方法は、上記の課題を解決するために、素数ｐ，ｑのうちｐを秘密鍵と

して生成し、その積ｎ＝ｐｑと、乱数ｓと、整数にｍｏｄｎの演算を施して得られる乗法群の最大生成源ｇとを用いて下記の関係式（１）で表されるｇ１を公開鍵として生成するとともに、入力された平文ｍに対して、上記公開鍵ｇ１、秘密鍵ｎおよび乱数ｒを用いて、下記の関係式（３）’で表される暗号文Ｃを生成することを特徴としている。

$g_1 = g^{s(p-1)} \pmod n$　・・・・・（１）

$C = m \cdot g_1^{r} \pmod n$　・・・・・（３）’

（ただし、情報ｂ＝size of ｐ（bits）であって、$0 < m < 2^{b-1}$，ｇｃｄ｛ｓ，ｑ－１｝＝１とする）。

【００７４】

上記の暗号化方法によれば、公開鍵として生成した鍵ｇ１は、（ｐ－１）のべき乗を含んでおり、公開鍵ｇ１及び秘密鍵ｎを用いて生成した暗号文Ｃも、（ｐ－１）のべき乗を含んでいるため、この暗号文Ｃを復号化する際において、フェルマーの小定理（$a^{p-1} \equiv 1 \pmod p$）を用いて、簡単に復号化することができる。

【００７５】

すなわち、本発明の暗号化方法は、２つの大きな素数ｐ，ｑを発生させ、これを秘密鍵として用いるとともに、この秘密鍵｛ｐ，ｑ｝と乱数ｓ，ｔとを用いて、それぞれ（ｐ－１）のべき乗を含むように公開鍵ｇ１を生成している。

【００７６】

さらに、秘密鍵ｐのサイズｂとの関係において、メッセージｍに長さの制限を課し、このサイズｂを用いることで、暗号文の生成および復号化の計算をそれぞれ１つの式で行うことができるため、中国人剰余定理を用いることなく、より簡単な計算により暗号化復号化処理を行うことができる。

【００７７】

また、本発明の暗号化方法によって生成された暗号文は、上記の暗号化方法と同様に、公開鍵ｇ１を用いて、（ｐ－１）のべき乗を含んだ式で表されるため、その復号化にはフェルマーの小定理を用いることが可能である。

【００７８】

フェルマーの小定理は、$a^{p-1} \equiv 1 \pmod p$で表され、（ｐ－１）のべき乗を含む数に対して、ｍｏｄｐの演算を施すことでその剰余を「１」に帰着させることができる。

【００７９】

よって、単純な秘密鍵｛ｐ，ｑ｝を用いて、簡単な計算で公開鍵ｇ１を生成し、暗号文も簡単な計算で算出でき、さらにこの暗号文の復号化についても、フェルマーの小定理を用いるだけで簡単に計算できるため、従来の暗号化方法と比較して、高速処理が可能になる。

【００８０】

一方、本発明の暗号化方法における安全性については、公開鍵ｇ１には、乱数ｓが含まれているため、公開鍵ｇ１及び秘密鍵ｎは互いに関係が断ち切られている。

【００８１】

よって、本発明の暗号化方法によれば、高い安全性を維持しつつ、計算量を減らして暗号化および復号化の高速処理を行うことが可能になる。

【００８２】

本発明の復号化方法は、上記の課題を解決するために、２つの素数ｐ，ｑを秘密鍵として生成し、その積ｎ＝ｐｑと、２つの乱数ｓ，ｔと、整数にｍｏｄｎの演算を施して得られる乗法群の最大生成源ｇとを用いて下記の関係式（１），（２）で表されるｇ１，ｇ２を公開鍵として用いるとともに、上記公開鍵｛ｇ１，ｇ２｝、秘密鍵ｎおよび乱数ｒ１，ｒ２を用いて、下記の関係式（３），（４）で表される平文ｍを暗号化した暗号文Ｃ＝（Ｃ１，Ｃ２）を受信し、フェルマーの小定理を用いて下記の関係式（５），（６）で表される受信暗号文ａ，ｂを生成し、該受信暗号文ａ，ｂから、中国人剰余定理を用いて、下記の関係式（７）を満たす平文ｍを導出し、復号化処理を行うことを特徴としている。

$g_1 = g^{s(p-1)} \pmod n$　・・・・・（1）
$g_2 = g^{t(q-1)} \pmod n$　・・・・・（2）
$C_1 = m \cdot g_1^{r1} \pmod n$　・・・・・（3）
$C_2 = m \cdot g_2^{r2} \pmod n$　・・・・・（4）
$a = C_1 \pmod p = m \pmod p$　・・・・・（5）
$b = C_2 \pmod q = m \pmod q$　・・・・・（6）
$m = aAq + bBp \pmod n$　・・・・・（7）
（ただし、$gcd\{s, q-1\} = 1$、$gcd\{t, p-1\} = 1$、$Aq \pmod p = 1$、$Bp \pmod q = 1$とする）

上記の復号化方法によれば、公開鍵として生成した鍵g_1，g_2は、それぞれ（$p-1$），（$q-1$）のべき乗を含んでおり、公開鍵$\{g_1, g_2\}$及び秘密鍵ｎを用いて生成した暗号文C_1，C_2も、（$p-1$），（$q-1$）のべき乗をそれぞれ含んでいるため、この暗号文C_1，C_2を復号化する際において、フェルマーの小定理（$a^{p-1} \equiv 1 \pmod p$）を用いて、簡単に復号化することができる。

【００８３】

すなわち、本発明の復号化方法においては、暗号文は、公開鍵$\{g_1, g_2\}$及び秘密鍵ｎを用いて、（$p-1$），（$q-1$）のべき乗を含んだ式で表されているため、その復号化にはフェルマーの小定理を用いることが可能になる。

【００８４】

フェルマーの小定理は、$a^{p-1} \equiv 1 \pmod p$で表され、（$p-1$）のべき乗を含む数に対して、ｍｏｄｐの演算を施すことでその剰余を「１」に帰着させることができる。

【００８５】

よって、暗号文C_1，C_2から、フェルマーの小定理を用いて、暗号文C_1，C_2に対応する２つの受信暗号文を算出し、ここでさらに中国人剰余定理を用いることで、２つの受信暗号文から平文ｍを復号化できる。

【００８６】

本発明の復号化装置は、以上のように、フェルマーの小定理を用いて簡単に暗号文を復号化できるため、従来の復号化方式と比較して、高速処理が可能になる。

【００８７】

本発明の復号化方法は、上記の課題を解決するために、素数ｐ，ｑのうちｐを秘密鍵として生成し、その積ｎ＝ｐｑと、乱数ｓと、整数にｍｏｄｎの演算を施して得られる乗法群の最大生成源ｇとを用いて下記の関係式（１）で表されるg_1を公開鍵として生成し、入力された平文ｍに対して、上記公開鍵g_1、秘密鍵ｎおよび乱数ｒを用いて、下記の関係式（３）’で表される暗号文Ｃを受信し、

フェルマーの小定理を用いて下記の関係式（８）を満たす平文ｍを導出し、復号化処理を行うことを特徴としている。

$g_1 = g^{s(p-1)} \pmod n$　・・・・・（1）
$C = m \cdot g_1^{r} \pmod n$　・・・・・（3）’
$m = C \pmod p$　・・・・・（8）
（ただし、$gcd\{s, q-1\} = 1$とする）

上記の復号化方法によれば、公開鍵g_1及び秘密鍵ｎを用いて生成した暗号文Ｃは、（$p-1$）のべき乗を含んでいるため、フェルマーの小定理（$a^{p-1} \equiv 1 \pmod p$）を用いて、この暗号文Ｃを簡単に復号化することができる。

【００８８】

すなわち、本発明の復号化方法は、秘密鍵ｐのサイズｂとの関係において、メッセージｍに長さの制限を課し、このサイズｂを用いることで、暗号文Ｃの生成および復号化の計算をそれぞれ１つの式で行うことができる。このため、中国人剰余定理を用いることなく、より簡単な計算により復号化処理を行うことができる。

【００８９】

また、本発明の復号化方法により復号化される暗号文は、公開鍵g_1及び秘密鍵nを用いて、（p－1）のべき乗を含んだ式で表されるため、その復号化にはフェルマーの小定理を用いることが可能である。

【００９０】

フェルマーの小定理は、$a^{p-1} \equiv 1$（ｍｏｄｐ）で表され、（p－1）のべき乗を含む数に対して、ｍｏｄｐの演算を施すことでその剰余を「１」に帰着させることができる。

【００９１】

よって、単純な秘密鍵｛p，q｝を用いて、簡単な計算で公開鍵g_1を生成し、暗号文も簡単な計算で算出でき、さらに暗号文の復号化についても、フェルマーの小定理だけを用いることで簡単に計算できるため、従来の復号化方式と比較して、さらに高速処理が可能になる。

【発明の効果】

【００９２】

本発明の暗号化方法、復号化方法を用いた暗号化装置、復号化装置、暗号システムによれば、高い安全性を維持しつつ、計算量を減らして暗号化および復号化の高速処理を行うことが可能になる。

【発明を実施するための最良の形態】

【００９３】

〔実施形態１〕

本発明の暗号化装置および復号化装置、並びにこれらを備えた暗号システム、暗号化方法および復号化方法に関する一実施形態について、図１および図２に基づいて説明すれば以下のとおりである。

【００９４】

本実施形態の暗号システムは、図２に示すような、基本的な概念に基づいて、メッセージ（平文）mの暗号化および復号化を行う。

【００９５】

すなわち、図２に示すように、メッセージ（平文）mに公開鍵｛g_1，g_2｝及び秘密鍵nを用いて、乱数Rを掛けて暗号文mRを生成し、これを相手先へ送信する。そして、暗号文mRを受信した者は、秘密鍵｛p，q｝を用いて乱数Rを「１」に帰着させ、メッセージmを復号する。

【００９６】

本実施形態の暗号システムは、図１に示すように、暗号化装置（暗号化演算手段）１１、通信路１４、および復号化演算装置（復号化演算手段）１５を備えている。

【００９７】

さらに、暗号化装置１１は、鍵生成部１２および暗号化演算装置１３を備えている。

【００９８】

鍵生成部１２は、メッセージmの暗号化および復号化に使用する公開鍵｛g_1，g_2｝と秘密鍵｛p，q｝とをそれぞれ生成する。なお、公開鍵｛g_1，g_2｝および秘密鍵｛p，q｝の生成については、後段にて詳述する。

【００９９】

暗号化演算装置１３は、入力されたメッセージmを公開鍵｛g_1，g_2｝及び秘密鍵nを用いて暗号文C_1，C_2を作成し、通信路１４へ出力する。

【０１００】

ここで、平文mは、m_1，m_2，m_3，…からなり、暗号文Cは、平文m_1を暗号化した暗号文C_1、平文m_2を暗号化した暗号文C_2、（以降同様）からなる。

【０１０１】

暗号文C_1は２つの乱数R_1、R_2を使った暗号文C_{11}およびC_{12}からなる。

【０１０２】

$C_1 = (C_{11}, C_{12})$

$C_{11}=m_1 R_1 \pmod n$
$C_{12}=m_1 R_2 \pmod n$
実際の暗号化の手順としては、まず、最初の平文m_1だけを暗号化した暗号文$C_1=(C_{11}, C_{12})$を作成し、それ以降の暗号文の作成については、平文m_2と２つの乱数R_1，R_2とを使用して暗号文を作成する。

【０１０３】

【数２】

$$C_2=m_2 \oplus R_j \quad (j=1 \text{or} 2)$$

【０１０４】

但し、ｊの値は、$m_1=(b_1 b_2 \cdots b_k)$のビット情報b_1に依存して決める。以降、C_3、C_4…についても同様に暗号化する。

【０１０５】

復号化演算装置１５は、通信路１４を介して暗号文C_1，C_2を受信するとともに、鍵生成部１２から秘密鍵｛ｐ，ｑ｝を受け取って、暗号文C_1、C_2からメッセージｍを復号して出力する。

【０１０６】

このように、公開鍵｛g_1，g_2｝を用いて、メッセージｍを暗号化して暗号文C_1，C_2として送信し、受信した側において、秘密鍵｛ｐ，ｑ｝を用いて暗号文C_1，C_2をメッセージｍに復号化することで、通信路１４におけるメッセージｍの漏洩、改竄等の問題の発生を防止して、安全性の高い通信を行うことができる。

【０１０７】

ここで、本実施形態の暗号システム１０によるメッセージｍの暗号化処理および復号化処理について説明すれば以下のとおりである。

【０１０８】

まず、鍵生成部１２による公開鍵｛g_1，g_2｝の生成について説明する。

【０１０９】

鍵生成部１２は、秘密鍵｛ｐ，ｑ｝（ｐ，ｑは大きな素数とする）、その積$n=pq$、ｇを整数×ｍｏｄｎの乗法群の最大生成源、ｓ，ｔをｇｃｄ｛ｓ，ｑ－１｝＝１，ｇｃｄ｛ｔ，ｐ－１｝＝１を満たす乱数とすると、公開鍵｛g_1，g_2｝を、以下の関係式（１）および関係式（２）で表される乱数として生成する。

$g_1=g^{s(p-1)} \pmod n$　・・・・・（１）
$g_2=g^{t(q-1)} \pmod n$　・・・・・（２）。

【０１１０】

ここで、上記関係式（１），（２）には、乱数ｓ，ｔが含まれているため、$n=pq$の式と上記関係式（１），（２）とは、完全に関係が断ち切られた状態となっている。よって、公開鍵｛g_1，g_2｝から秘密鍵｛ｐ，ｑ｝を導き出すためには、２つの大きな素数ｐ，ｑの積である「ｎ」から素因数分解によってｐ，ｑを導き出す必要がある。

【０１１１】

続いて、暗号化演算装置１３による上記関係式（１）および関係式（２）で表される公開鍵｛g_1，g_2｝を用いたメッセージｍの暗号文の作成について説明する。

【０１１２】

ｍをメッセージ（平文）（但し、$m<n$とする）、r_1，r_2を乱数、暗号文を$C=(C_1, C_2)$とすると、暗号文$C=$｛C１，C_2｝は、公開鍵｛g_1，g_2｝及び秘密鍵ｎを用いて、以下に示す式によって表される。

$C_1=m \cdot g_1^{r_1} \pmod n$　・・・・・（３）
$C_2=m \cdot g_2^{r_2} \pmod n$　・・・・・（４）。

【０１１３】

暗号文Ｃには、上記関係式（３）、関係式（４）に示すように、乱数g_1，g_2の乱数r_1，r_2が含まれているため、メッセージｍを乱数として相手先に送信できる。

【０１１４】
なお、上記関係式（３）および関係式（４）の$g_1{}^{r_1}$，$g_2{}^{r_2}$が、図２に示す概念図における乱数Ｒに相当する。
【０１１５】
そして、復号化演算装置１５による暗号文C_1，C_2からメッセージｍへの復号化について説明する。
【０１１６】
復号化演算手段１５は、秘密鍵｛ｐ，ｑ｝を用いて、暗号文C_1，C_2をメッセージｍに復号化する。
【０１１７】
ここで、本発明の暗号システムでは、メッセージｍを復号化する際に、先ず、フェルマーの小定理（$a^{p-1}\equiv 1\ (\mathrm{mod}\ p)$）を用いて、（ｐ－１）のべき乗が含まれている乱数部分を「１」に帰着させることができるため、以下に示す受信暗号文ａ，ｂが生成される。
$a=C_1\ (\mathrm{mod}\ p)=m\ (\mathrm{mod}\ p)$　・・・・・（５）
$b=C_2\ (\mathrm{mod}\ q)=m\ (\mathrm{mod}\ q)$　・・・・・（６）。
【０１１８】
ここで、上記関係式（５）および関係式（６）の右辺について、ｍ＞ｐ、ｍ＞ｑであるため、ｍ（ｍｏｄｐ）およびｍ（ｍｏｄｑ）は乱数であり、メッセージｍは完全に復号されていない。
【０１１９】
そこで、本発明の暗号システムでは、上記２つの関係式（５）および関係式（６）に基づいて、中国人剰余定理を用いてメッセージｍを復号する。
【０１２０】
すなわち、中国人剰余定理を用いれば、メッセージｍは、上記関係式（５）および関係式（６）に基づいて以下の関係式（７）によって表されるため、復号化されたことがわかる。
$m=aAq+bBp\ (\mathrm{mod}\ n)$・・・・・（７）
（ただし、$Aq\ (\mathrm{mod}\ p)=1$，$Bp\ (\mathrm{mod}\ q)=1$とする）。
【０１２１】
本発明の暗号システムは、以上のように、フェルマーの小定理を用いて復号化することができるように、（ｐ－１）乗、（ｑ－１）乗を含むように公開鍵｛g_1，g_2｝を生成し、復号化の際には、フェルマーの小定理および中国人剰余定理を用いてメッセージｍを復号化する。
【０１２２】
これにより、非常に簡単な計算で公開鍵｛g_1，g_2｝を生成できるため、極めて簡単な暗号系を提案できる。また、２つの大きな素数ｐ，ｑをそのまま秘密鍵｛ｐ，ｑ｝として用いることができる。さらに、フェルマーの小定理と中国人剰余定理とを用いて簡単な計算によりメッセージｍを復号できるため、従来のＲＳＡ暗号システムと比較して、暗号化する際の計算量を減らして、高速処理が可能な暗号システムを得ることができる。
【０１２３】
〔実施形態２〕
本発明の暗号化装置および復号化装置、並びにこれらを備えた暗号システム、暗号化方法および復号化方法に関する他の実施形態について説明すれば、以下のとおりである。
【０１２４】
本実施形態の暗号システムは、上記実施形態１の暗号システムと基本的な原理については同様であるが、秘密鍵ｐのサイズｂをメッセージｍとの関係で制限することを条件として、アルゴリズムをより単純化することができる。
【０１２５】
すなわち、上記実施形態１の暗号システムでは、１つのメッセージｍに対して、２つの

暗号文C_1，C_2を生成しているが、本実施形態の暗号システムでは、秘密鍵ｐのサイズｂを$0<m<2^{b-1}$という条件式を満たすように制限し、このサイズｂを用いることで、１つの暗号文Ｃを生成し、これを復号するだけで済むため、より暗号化、復号化処理を高速化が図れる。

【０１２６】

具体的には、暗号化演算装置は、乱数ｒを発生させるとともに、秘密鍵ｐのサイズｂと、秘密鍵ｐとを用いて下記の関係式（１）で表される公開鍵ｇと、（３）’で表される暗号文Ｃを生成する。

$g_1=g^{s(p-1)}\ (\mathrm{mod}\ n)$　・・・・・（１）

$C=m\cdot g_1^{r}\ (\mathrm{mod}\ n)$　・・・・・（３）’

（ただし、メッセージｍとサイズｂとは、$0<m<2^{b-1}$の条件式を満たす）。

【０１２７】

続いて、上記暗号文Ｃの復号化については、上記実施形態１の暗号システムと同様に、復号化演算装置が、フェルマーの小定理（$a^{p-1}\equiv 1\ (\mathrm{mod}\ p)$）を用いて、下記の関係式（８）を導出する。

$m=C\ (\mathrm{mod}\ p)$　・・・・・（８）。

【０１２８】

ここで、暗号文Ｃには、g_1が含まれており、実施形態１のg_1の関係式（１）より、g_1は（ｐ－１）乗を含んでいるため、（ｍｏｄｐ）をとることにより、ｍ以外の数を１に帰着させることができるため、メッセージｍを容易に復号化できる。

【０１２９】

本実施形態の暗号システムでは、以上のように、秘密鍵ｐのサイズｂについてメッセージｍとの関係で制限する。そして、公開鍵g_1を生成して、１つの暗号文Ｃを生成し、この暗号文Ｃを秘密鍵ｐを用いて復号するため、実施形態１で用いた中国人剰余定理を用いなくても容易に復号化処理を行うことができる。

【０１３０】

よって、上記実施形態１の暗号システムと等価の安全性を維持しつつ、実施形態１の暗号化装置よりもさらに高速処理が可能な暗号システムを得ることができる。

【０１３１】

また、上述した本実施形態の暗号システムは、以下のような特徴を有している。

【０１３２】

１つ目の特徴としては、暗号文C_1，C_2を示す上記関係式（３），（４）には、$g_1^{r_1}$が含まれているため、メッセージｍを送るたびに暗号文が異なる、いわゆる確率暗号となっている。これは、べき乗の「ｒ」が乱数であることによる特徴である。よって、ＲＳＡ暗号化方式では、メッセージｍと暗号文Ｃとが一対一に対応するのに対し、本発明の暗号システムでは、メッセージｍと暗号文Ｃとが一対一に対応しないため、暗号文Ｃから解読することが困難であり、より暗号強度を高めることができる。

【０１３３】

２つ目の特徴としては、メッセージｍから暗号文Ｃへの変換は容易であるが、その逆の変換は非常に困難である、いわゆる一方向性関数であることが挙げられる。

【０１３４】

３つ目の特徴としては、１つ目の特徴としてあげたように、メッセージｍと暗号文Ｃとが一対一に対応しないため、生成された暗号文が同じ暗号文Ｃであっても、元のメッセージが異なるメッセージm_0，m_1である可能性がある。よって、暗号文Ｃからは、どのメッセージｍを暗号化したものかわかりにくいため、暗号強度を高めることができる。

【０１３５】

ここでさらに、暗号解析者による以下に示す３種類の攻撃に対する本発明の暗号システムの安全性について説明すれば以下のとおりである。

【０１３６】

まず、１つ目の攻撃として、選択平文攻撃（Chosen Plaintext Attack：ＣＰＡ）に対

する安全性について説明する。

【０１３７】

この選択平文攻撃は、通常、暗号文を作成する際のプロセスであり、与えられた平文（メッセージ）mに対する暗号文のペアを多数作成し、新しい暗号文が与えられた際に平文を求めることができるか否かについて調べることで、暗号文を復号する鍵を求める攻撃である。

【０１３８】

これに対し、本発明の暗号システムは、上述のように、一方向性関数であって、かつ確率暗号であるため、メッセージmと暗号文Ｃとが一対一に対応していない。このため、この選択平文攻撃に対する本発明の暗号システムの安全性は高いことがわかる。

【０１３９】

２つ目の攻撃として、非適応型選択暗号文攻撃（Non-Adaptive Chosen Ciphertext Attack：ＣＣＡ１）に対する安全性について検討する。

【０１４０】

この非適応型選択暗号文攻撃は、暗号文を与えてこれに対応する平文のペアを作成し、ターゲットとなる暗号文を与えて平文が求められるかを調べる攻撃であって、かつ復号化したいターゲットとなる暗号文に質問した後は一切質問不可となる条件の攻撃である。

【０１４１】

これに対して、本発明の暗号システムは、上記と同様に、一方向性関数であって、かつ確率暗号であるため、メッセージmと暗号文Ｃとが一対一に対応していない。このため、この非適応型選択暗号文攻撃に対する本発明の暗号システムの安全性は高いことがわかる。

【０１４２】

３つ目の攻撃として、適応型選択暗号文攻撃（Adaptive Chosen Ciphertext Attack：ＣＣＡ２）に対する安全性について説明する。

【０１４３】

この適応型選択暗号文攻撃は、暗号文を与えてこれに対応する平文のペアを作成し、ターゲットとなる暗号文を与えて平文が求められるかを調べる攻撃であって、かつ復号化したいターゲットとなる暗号文以外は何をいつ聞いてもよいという条件で、前回の結果を活用して繰り返し処理を行う攻撃である。

【０１４４】

これに対して、本発明の暗号システムは、ターゲットとなる暗号文が識別不能であるため、完全に安全であるとは言い難い。

【０１４５】

つまり、ターゲットとなる暗号文Ｃ＝（C_1，C_2）とすると、C_1，C_2は以下に示すようになる。

$C_1 = m \cdot g_1^{r_1} \pmod n \Rightarrow C_1^* = m \cdot g_1^{r_1 + t_1} \pmod n$

$C_2 = m \cdot g_2^{r_2} \pmod n \Rightarrow C_2^* = m \cdot g_2^{r_2 + t_2} \pmod n$

ここで求めた$C^* = (C_1^*, C_2^*)$は$C^* \neq C$であるが、C^*を提示して平文mを得ることができるため、本発明の暗号システムは、この適応型選択暗号文攻撃に対しては安全ではないといえる。

【０１４６】

そこで、本実施形態の暗号システムでは、適応型選択暗号文攻撃に対して耐性を持たせるために、Ｃ＝（C_1，C_2，ｅ）とする。

【０１４７】

ただし、「ｅ」は、$C_1 = m \cdot g_1^{r_1} \pmod n$，$C_2 = m \cdot g_2^{r_2} \pmod n$）より、ｄ＝（$C_1 + C_2$）／ｍ（ｍｏｄｎ）であるから，ｅ＝ｈ（ｄ）（ｈは一方向性ハッシュ関数）とする。

【０１４８】

これにより、暗号文Ｃは長くなるという問題はあるが、ｅを３２bitsまたは６４bitsに

まとめることができるとともに、メッセージｍが少しでも変わるとｅが一致しなくなるため、上記適応型選択暗号文攻撃に対して耐性を持たせて、信頼度の高い暗号システムを得ることができる。

【０１４９】

なお、本発明の暗号システムは、以下に示すデータベースを用いることにより、演算をより高速化できる。

$DB(2, e) = [R_{ij} = g_i^{r_{ij}} \pmod n]$

（ただし、$1 \leqq i \leqq 2$，$1 \leqq j \leqq e$）

$C = (C_1, C_2)$

【０１５０】

【数１】

$$C_1 = m \cdot \prod_{k=1}^{\delta 1} R_{1,jk} \pmod n$$

$$C_2 = m \cdot \prod_{l=1}^{\delta 2} R_{2,jl} \pmod n$$

【０１５１】

すなわち、２行×ｅ列のデータベースにR_{ij}を前もって計算して蓄積しておくことで、暗号化処理を行う際には、このデータベースからR_{ij}を取り出して乱数部分を作ることができるため、暗号化処理をより高速化できる。

【０１５２】

これにより、例えば、計算量が多い従来のＲＳＡ暗号方式と比較して、暗号化処理を高速化できるとともに、復号化処理についてはｍｏｄｐの演算を施すことだけで復号化できるため、計算量が多いＲＳＡ暗号化方式と比較してはるかに高速化できる。

【０１５３】

さらに、本発明の暗号システムは、べき乗の特性を利用して、図３に示すような拡張ブロックサイファに応用することができる。

【０１５４】

この拡張ブロックサイファは、暗号文C_1だけを通常のスキルで暗号文C_{11}，C_{12}に暗号化し、後のC_2以降の暗号文については前の暗号文C_{11}，C_{12}に含まれる２つの乱数R_1，R_2を使用して暗号文を作成するため、従来の共通鍵暗号系と公開鍵暗号系とで処理をより高速化できる。

【０１５５】

具体的には、最初の暗号文C_1についてのみ通常の手順で暗号文C_{11}，C_{12}を作成し、C_2以降の暗号文については、最初のビット$b_i = 0$の場合には、R_1を加算し、最初のビット$b_i = 1$の場合には、R_2を加算していくことで、暗号文Ｃを作成できる。

【０１５６】

【表１】

《暗号化》

	べき乗計算	かけ算
Original	2	2
Extended	2／k	2／k

単位(回)

《復号化》

	割り算	かけ算
Original	2	2
Extended	4/k	2／k

単位(回)

【０１５７】

表１は、図３に示す拡張ブロックサイファによって計算回数をどれだけ減らせるかを示している。

【０１５８】

暗号化処理については、表１上段に示すように、ブロック長ｋとすると、べき乗計算、掛け算ともに、計算回数を２／ｋ回に減らせることが分かる。

【０１５９】

復号化処理については、表１下段に示すように、ブロック長ｋとすると、割り算については４／ｋ回に、掛け算については２／ｋ回に減らせることが分かる。

【０１６０】

以上のように、本発明の暗号システムの応用例として、拡張ブロックサイファを適用することで、より計算回数の少ない高速処理が可能なハイブリッド型の暗号システムを得ることができる。

【０１６１】

なお、上記実施形態２の単純化した暗号システムにこの拡張ブロックサイファを適用した場合には、表１に示す計算回数は全て１回になり、非常に使い易い暗号システムが得られる。

【０１６２】

さらに、本発明の暗号システムをディジタル署名に適応させた場合について説明すれば以下のとおりである。

【０１６３】

まず、公開鍵 $\{g_1, g_2\}$ の指数部分ｓ（ｐ－１）とｔ（ｑ－１）とをα、βとすると、署名（ｕ，ｖ）は以下の式で表される。

$u = \alpha r + \beta m \pmod{\Phi(n)}$　・・・・・（１２）

$v = g^{(\alpha^2 r + \beta^2)} \pmod{n}$　・・・・・（１３）

（ただし、メッセージm，m≦Me≦Φ（n），乱数rとする）。

【０１６４】

上記関係式（１２）より、uには不明な変数が３つ以上あるため、この式を解くことはできない。また、上記関係式（１３）より、vでは、g，α，β，rは全て秘密の変数であるため、この式を解くこともできない。

【０１６５】

また、この署名付きメッセージ｛m，（u，v）｝の認証式は、以下の関係式で表される。

$(g_1{}^m g_2)^u = v^m \pmod n$　・・・・・（１４）。

【０１６６】

続いて、この関係式（１４）を認証する。

【０１６７】

$$(g_1{}^m \cdot g_2)^u = g^{(\alpha m+\beta)(\alpha r+\beta m)} \pmod n$$
$$= g^{(\alpha^2 r+\beta^2)m} \pmod n$$
$$= v^m \pmod n$$

（ただし、$g^{\alpha\beta} = g^{stΦ(n)} = 1 \pmod n$とする）。

【０１６８】

これにより、署名した人から送信されたメッセージmであることが認証された。

【０１６９】

本発明の暗号システムは、以上のように、従来とは異なる新たな方式であって、安全性が高く、高速処理が可能なディジタル署名を提案できる。

【０１７０】

なお、本発明の暗号化装置および復号化装置、並びにこれらを備えた暗号システム、暗号化方法および復号化方法は、例えば、相手認証、相互認証、電子選挙および電子入札等にも適用することができる。

【０１７１】

また、本発明の暗号システムは、２つの大きな素数p，qを秘密鍵として用いるとともに、素数p，qについてその積n＝pqと、（p－１）および（q－１）のべき乗および乱数s、tを含むg_1，g_2とを公開鍵｛g_1，g_2｝、秘密鍵nとして、暗号文C＝（C１，C２）を作成する暗号化装置と、該暗号文Cに対してフェルマーの小定理を用いて暗号文Cを復号化する復号化装置とを備えていることを特徴とする暗号システムと、関係式を用いることなく表現することもできる。

【０１７２】

なお、本発明の暗号化技術は、例えば、家庭内の小さな領域でのストリーミングデータのスクランブラあるいはデスクランブラに適用することが可能である。

【０１７３】

また、本発明は、暗号鍵の配布に適用することも可能である。

【０１７４】

本発明は上述した各実施形態に限定されるものではなく、請求項に示した範囲で種々の変更が可能であり、異なる実施形態にそれぞれ開示された技術的手段を適宜組み合わせて得られる実施形態についても本発明の技術的範囲に含まれる。

【図面の簡単な説明】

【０１７５】

【図１】本発明の暗号化装置および復号化装置、並びにこれらを備えた暗号システム、暗号化方法および復号化方法の一実施形態を示す暗号システムの構成を示すブロック図である。

【図２】本発明の暗号化および復号化処理の概念を簡潔に示すブロック図である。

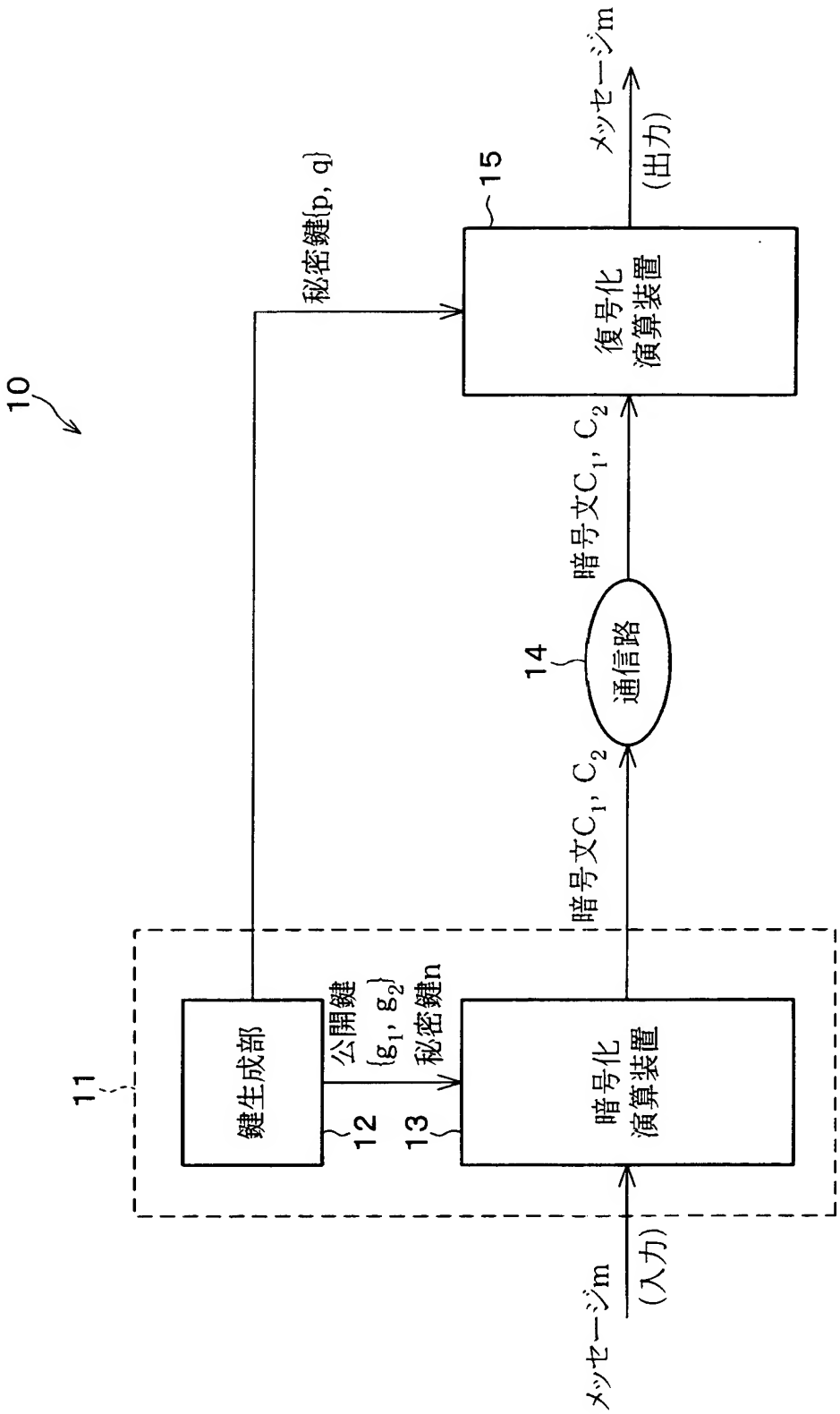
【図３】本発明の暗号システムの応用例としての拡張ブロックサイファの態様を示す図である。

【符号の説明】

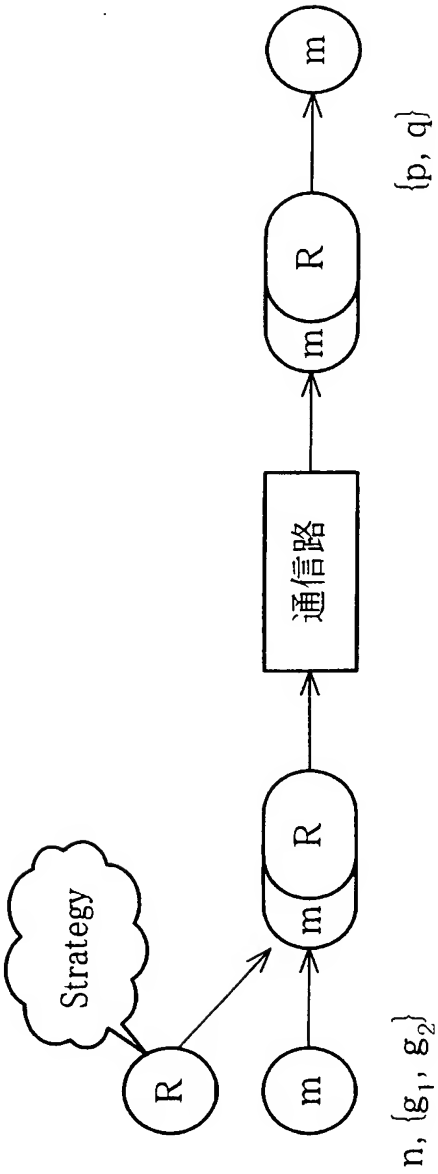
【０１７６】

１０　暗号システム
１１　暗号化装置
１２　鍵生成部
１３　暗号化演算装置
１４　通信路
１５　復号化演算装置
ｍ　メッセージ（平文）
ｎ　秘密鍵（２つの大きな素数の積）
g_1，g_2　公開鍵
ｐ，ｑ　秘密鍵（２つの大きな素数）
Ｃ　暗号文
C_1，C_2　暗号文

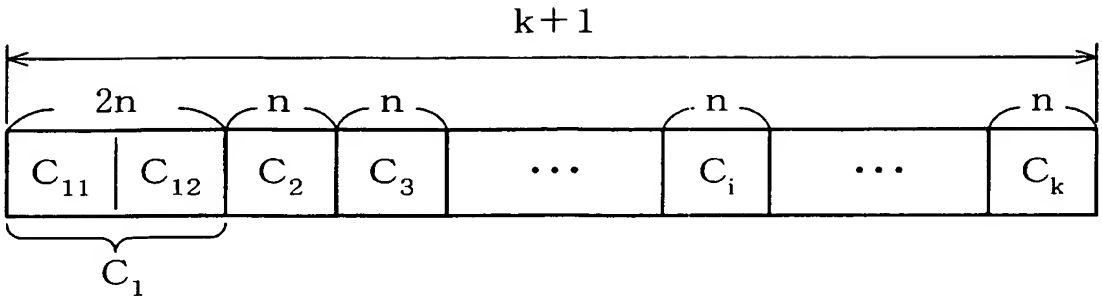
【書類名】図面
【図１】


10
11
鍵生成部
12
公開鍵
{g1, g2}
秘密鍵n
13
暗号化
演算装置
メッセージm
(入力)
暗号文C1, C2
14
通信路
暗号文C1, C2
秘密鍵{p, q}
15
復号化
演算装置
メッセージm
(出力)

【図２】



【図３】



$C_1=(C_{11}, C_{12})$, $C_{11}=m_1R_1(\mathrm{mod}\ n)$, $C_{12}=m_1R_2(\mathrm{mod}\ n)$

$C_i=m_i \oplus R_{b_i+1}$; $b_i=0\mathrm{or}1 \in m_1$, $2 \le i \le k < \lfloor \log_2 n \rfloor$

【書類名】要約書
【要約】
【課題】　極めて簡単な暗号系を提案し、ＲＳＡ暗号化方式と等価な安全性を保持しつつ、暗号化および復号化する際の計算量を減らして単純化し、簡単な計算で暗号化および復号化が可能な暗号化装置および復号化装置、並びにこれらを備えた暗号システム、暗号化方法および復号化方法を提供する。
【解決手段】　暗号システム１０は、暗号化装置１１、通信路１４、および復号化演算装置１５を備えている。暗号化装置１１の鍵生成手段１２は、公開鍵｛g_1，g_2｝を、（ｐ－１）、（ｑ－１）のべき乗を含む乱数として生成し、復号化の際には、フェルマーの小定理および中国人剰余定理を用いてメッセージｍを復号化する。
【選択図】　図１

特願２００４－０１３４０１

出　願　人　履　歴　情　報

識別番号　　［０００００５０４９］

１．変更年月日　　１９９０年　８月２９日
［変更理由］　　新規登録
住　所　　大阪府大阪市阿倍野区長池町２２番２２号
氏　名　　シャープ株式会社

特願２００４－０１３４０１

出　願　人　履　歴　情　報

識別番号　［５０３０３４６２９］

１．変更年月日　２００３年　１月２４日
［変更理由］　新規登録
住　所　兵庫県神戸市須磨区中落合４丁目２－４６７－３０２
氏　名　田中　初一